# The FBCA Testing and the EMA Challenge

Tim Polk

NIST PKI Team

# Problem

- Agency PKIs are developed as independent trust domains
  - initially designed to support intra-agency applications
- Goal: Support interagency PKI interoperability
  - technical interoperability
  - policy interoperability

# Background

- FBCA is non-hierarchical, peer-to-peer “hub” - not a “root”
- Supports interagency PKI technical interoperability by establishing certification paths
- Supports policy interoperability as determined by the FPKI Policy Authority
- Intended to accommodate Federal agency use of any PKI COTS product

# Federal Bridge Certification Authority

- Current Status
- Testing and Demonstration
- Participants
- Results
- Conclusions and lessons learned
- Remaining challenges

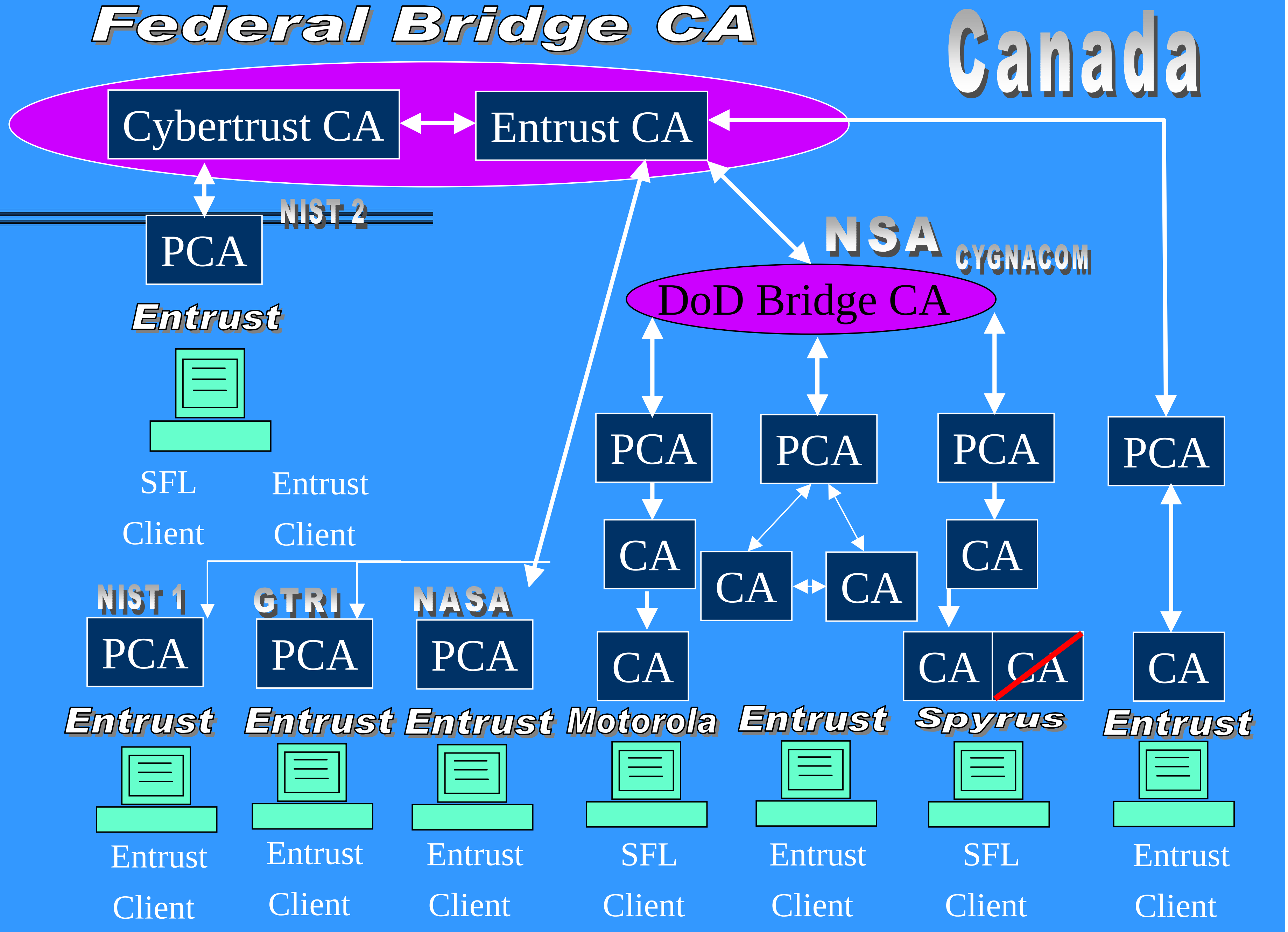
# Current Status

- Prototype FBCA operational 2/8/00
  - GSA auspices; hosted by Mitretek Systems
  - Entrust and Cybertrust CAs
  - PeerLogic i500 directory
  - Supports EMA Challenge and testing
- Production FBCA operational late 2000
  - Additional CA products within membrane
  - Mesh arrangement within membrane

# Test Structure

- Six disparate PKI domains cross-certified with FBCA
  - Five different CA products
  - Five different X.500 directory products
- Interoperability demonstrated via exchange of signed S/MIME messages
- X.500 directory framework - chaining between directories, client access via LDAP

# Federal Bridge CA



Canada

Cybertrust CA

Entrust CA

NIST 2

PCA

Entrust

SFL Client

Entrust Client

NSA

CYGNACOM

DoD Bridge CA

PCA

PCA

PCA

PCA

CA

CA

CA

CA

NIST 1

GTRI

NASA

PCA

PCA

PCA

CA

CA

~~CA~~

CA

Entrust

Entrust

Entrust

Motorola

Entrust

Spyrus

Entrust

Entrust Client

Entrust Client

Entrust Client

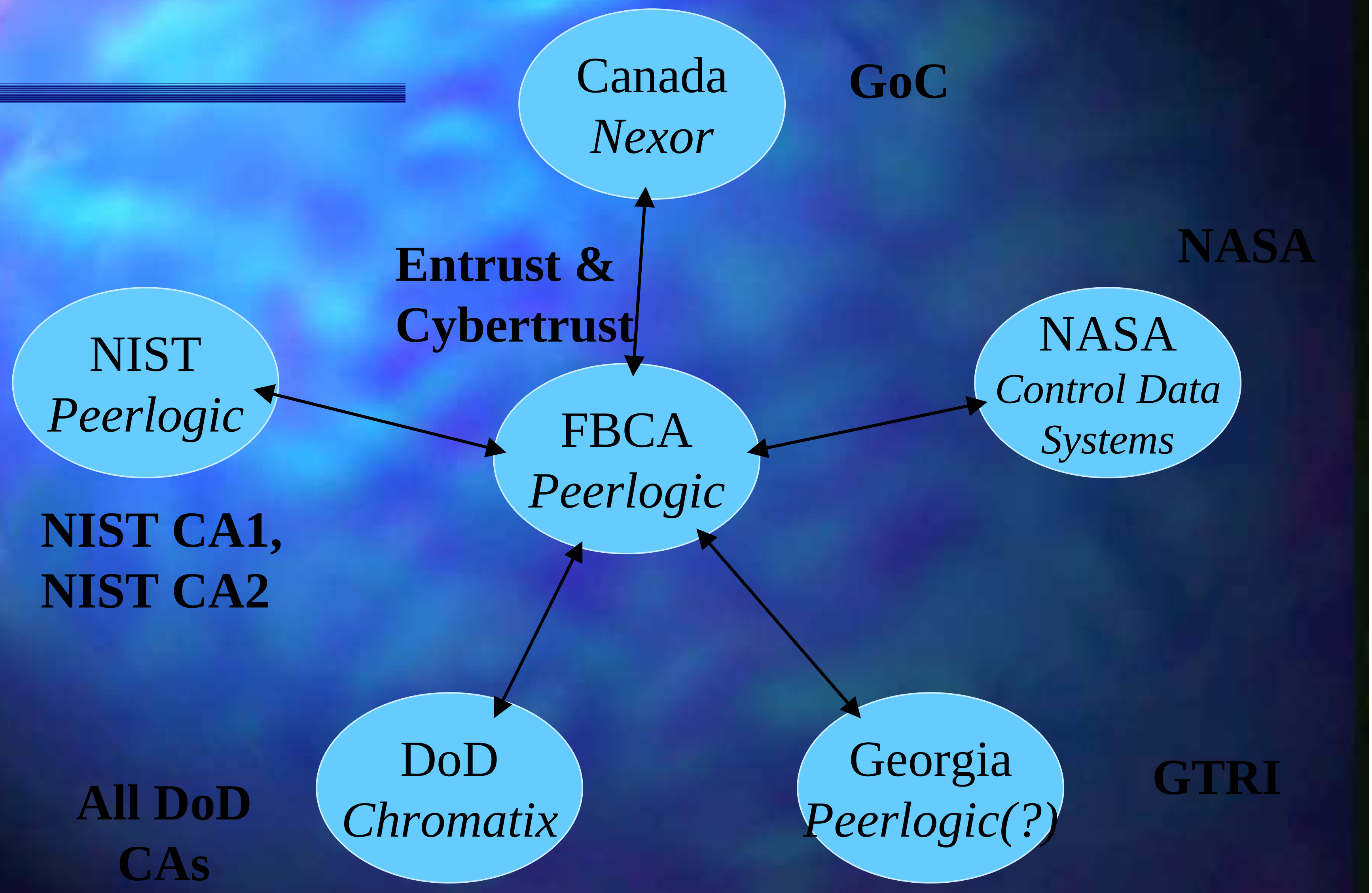
SFL Client

Entrust Client

SFL Client

Entrust Client

# Directory Configuration



Canada

*Nexor*

GoC

Entrust & Cybertrust

NASA

NIST

*Peerlogic*

FBCA

*Peerlogic*

NASA

*Control Data Systems*

NIST CA1, NIST CA2

DoD

*Chromatix*

Georgia

*Peerlogic(?)*

All DoD CAs

GTRI

# Client Details

- Eudora engineered with:
  - Entrust toolkit (“out of the box”)
  - CygnaCom libraries
  - JGVanDyke libraries
- Spyrus LYNKS cryptocards for CygnaCom/JGVanDyke enabled client
- Private key on hard disk for Entrust enabled client

# Participants

- Government of Canada
- NSA/DOD
- NIST
- NASA
- GSA
- Georgia Tech Research Institute

- CA products: Entrust; Cybertrust; CygnaCom; Spyrus; Motorola
- Directories: PeerLogic; ICL; Nexor; CDS; Chromatix
- Integrators: Mitretek; JGVanDyke; GNS; Booz Allen; CygnaCom; A&N Associates

# Results

| From<br>To | NIST CA#1 | NIST CA#2 | DOD Entrust | DOD Spyrus | DOD Mot. | Canada | GTRI | NASA | GSA |
|---|---|---|---|---|---|---|---|---|---|
| NIST CA#1 | NA | ▨ | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | 🟩 | CUD |
| NIST CA#2 | ▨ | NA | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | CUD |
| DOD Entrust | 🟩 | ▨ | NA | NA | NA | 🟩 | 🟩 | 🟩 | CUD |
| DOD Spyrus | 🟩 | 🟦 | NA | NA | NA | 🟩 | 🟩 | 🟩 | CUD |
| DOD Mot. | 🟩 | 🟦 | NA | NA | NA | 🟩 | 🟩 | 🟩 | CUD |
| Canada | 🟩 | ▨ | 🟩 | DEB | DEB | NA | 🟩 | 🟩 | CUD |
| GTRI | 🟩 | ▨ | 🟩 | 🟩 | 🟩 | 🟩 | NA | 🟩 | CUD |
| NASA | 🟩 | ▨ | 🟩 | DEB | DEB | 🟩 | 🟩 | NA | CUD |
| GSA | CUD | CUD | CUD | CUD | CUD | CUD | CUD | CUD | CUD |

# Conclusions and Lessons Learned

- FBCA concept works
- Client ability to develop and process trust path straightforward to implement
- Directory interoperability is **critical** to PKI interoperability
- Directory entries must line up with CAs
- Lots of details, lots of devils

# Challenges Ahead For the FBCA

- Continue testing
  - Achieve interoperability between all domains
  - Test encryption and policy mapping
- Proceed to develop production FBCA
  - Stand up FPKI Policy Authority under Federal CIO Council
- Vendor Outreach
  - Need ubiquitous support for trust path creation and processing